GRAND DUCHY OF LUXEMBOURG
Ministry of Foreign Affairs

Directorate for Development Cooperation

European Union Africa
Infrastructure Trust Fund

Trafic et analyse des flux de données pour les réseaux IP

Internet Society™

Remerciements et Attribution

Cette présentation contient du contenu et des informations initialement développés et maintenus par les organisations suivantes / personnes et prévu pour le projet de l'Union africaine AXIS

Mark Tinka: - mtinka@psg.org

Aperçu de la présentation

- A propos des flux
- Comment les flux sont accessibles
- Comment analyser les flux
- Quelle est l'utilité des données de flux

A propos des flux

A propos des flux

- Les flux de trafic:
  - Une séquence de paquets.
  - Échangées entre les sources discrètes + destinations.

  - Les données de flux ne sont pas nécessairement une correspondance 1:1.
  - Peut aussi être un groupe de paquets dans le réseau.

Comment les flux sont accessibles

Comment les flux sont accessibles

- Trois méthodes bien connues aujourd'hui:
  - NetFlow (et ses amis)
  - IPFIX
  - sFlow

Comment les flux sont accessibles

- NetFlow:
  - Initialement développé par Cisco Systems.
  - Développé pour capturer des informations de trafic IP.

  - La plupart des implémentations courantes sont NetFlow v9 v5 +.
  - NetFlow v9 ajoute le support pour les données MPLS et IPv6..

  - Les données suivantes peuvent être tirées de flux:
    - Données SNMP.
    - Adresses IP.de Source + destination
    - Protocole IP.
    - Source UDP+ TCP + Informations de destination.
    - IP ToS données.

Comment les flux sont accessibles

- Amis NetFlow:
  - Plusieurs fournisseurs ont développé NetFlow.
  - Sont appelés par d'autres noms, mais sont les mêmes.

  - Les autres implémentations sont les suivants:
    - AppFlow – Citrix.
    - Cflowd – Alcatel Lucent.
    - JFlow/cflowd – Juniper.
    - NetStream – 3Com.
    - NetStream – Huawei.
    - Rflow – Ericsson.
    - sFlow – Allied Telesis.

Comment les flux sont accessibles

- IPFIX:
  - Exportation de l' information sur le Flux d'Internet Protocol
  - Un protocole basé sur la norme de débit de capture.

  - Est basé sur Cisco NetFlow v9.
  - Développé pour tout système qui nécessite des captures de flux.

  - IPFIX utilise SCTP comme protocole de transport.
  - Mais prend également en charge les protocoles TCP et UDP.

Comment les flux sont accessibles

- sFlow:
  - Capture d'un échantillon de tous les "paquets" sur le réseau.
  - Désignation de la technologie est un terme impropre.
  - sFlow ne tient pas compte des flux. Il capture des paquets.

  - Utilisé principalement sur les commutateurs de couche 2 informations.

Comment les flux sont accessibles

- NetFlow / IPFIX Différences avec sFlow:
  - Avec NetFlow, cache de flux est construit sur le routeur.
  - Avec NetFlow, cache de flux est construit sur le routeur.

  - Avec sFlow, têtes de paquets exportés immédiatement.
  - Avec NetFlow, les dispositifs sont complexes, coûteuses.

  - Avec sFlow, les appareils sont plus simples, moins chers.
  - sFlow paquets d'échantillons, ce qui est moins précis.

  - NetFlow permet une certaine souplesse ensemble de données.
  - sFlow seulement des échantillons de paquets.

Comment analyser les flux

Comment analyser les flux

- Trois étapes dans l'analyse des flux:
  - Recueillir les flux.
  - Exporter les flux.
  - Analyser les flux.

- Dans certains cas:
  - Débit d'exportation n'est pas vraiment nécessaire.
  - Collection + analyse peut se faire localement.
  - Non extensible, mais peut être un "quick & dirty" fix.

Comment analyser les flux

- Recueillir les flux:
  - Périphérique doit prendre en charge une mise en œuvre NetFlow..
  - NetFlow configuré sur la participation des interfaces.
  - Débit du cache est construit sous forme de données et traverse le dispositif.

Comment analyser les flux

- Exporter les flux:
  - Ressources du périphérique sont limitées.
  - Appareils construits pour commutation / routage, pas l'analyse des flux.
  - Ainsi, les flux peuvent être exportés vers un analyseur dédié.

  - Cache Débit construit sur un dispositif local.
  - Les données de flux, puis exportées vers un analyseur dédié.
  - Données sur les flux d'exportation envoyée périodiquement (configurable).

  - Les données pourraient être non échantillonnés (précis, mais infranchissable).
  - Les données peuvent être échantillonnés (moins précis, mais évolutive).

Comment analyser les flux

- Analyser les flux:
  - Données sur les flux exportés est cru.
  - Doit être analysé pour plus de commentaires.
  - Analyseurs peut générer beaucoup d'informations provenant de l'écoulement.

  - Les résultats peuvent être représentés de différentes façons.
  - Sous forme de graphiques ou de tableaux.

  - Flexibilité représentation varie.
  - Sur la base d'un analyseur et de fonctionnalités.

Comment analyser les flux

- Deux grands types d'analyseurs de flux:
  - Non commerciaux et / ou libre.
  - Commerciaux et / ou payants.

Comment analyser les flux

- Non commerciaux et / ou payants:
  - Basé sur Linux / UNIX ou Windows.
  - Fournit des rapports raisonnables.
  - Bon pour les réseaux de petite ou moyenne taille.
  - Pas fort sur les fonctionnalités.
  - par exemple, Flow-outils, Nfsen / nfdump, E.T.C.

Comment analyser les flux

- commerciaux et / ou payants
  - Basé sur des systèmes propriétaires et de la technologie.
  - Généralement très coûteux.
  - Sont très compétents et ont des fonctionnalités étendues.
  - Très flexible, offrant des options de rapports divers.
  - par exemple, Arbor Networks, Network Instruments, E.T.C.

Quelle est l'utilité des données de flux

Quelle est l'utilité des données de flux

- Plusieurs utilisations légitimes:
  - La facturation des clients.
  - En amont et en profilage peering.
  - détection DoS/DDoS.
  - atténuation DoS/DDoS (avec extensions).
  - IPv6 suivi de la croissance du trafic.
  - Visibilité sur les données de couche 2, par exemple, MPLS, Ethernet, etc

GRAND DUCHY OF LUXEMBOURG
Ministry of Foreign Affairs

Directorate for Development Cooperation

European Union Africa
Infrastructure Trust Fund

END

Internet Society™